CZU: [004.056 + 007]:659.3

SECURITATEA CIBERNETICĂ ÎN ECOSISTEMUL MASS-MEDIA: DINAMICI TEHNOLOGICE ȘI IMPLICAȚII PRIVIND PROTECȚIA DATELOR

CYBER SECURITY IN THE MASS MEDIA ECOSYSTEM: TECHNOLOGICAL DYNAMICS AND IMPLICATIONS FOR DATA PROTECTION

Mariana TACU,
doctor în științe politice, conferențiar universitar
Universitatea de Stat din Moldova
ORCID: 0000-0003-4930-2395,
mariana.tacu@usm.md

Progresul tehnologic a condiționat multiaspectual procesul de transfigurare digitală al mass-mediei, pe de o parte modificând structura acestei industrii, pe de altă parte redefinind modalitățile de informare și distribuire a conținutului. Odată cu aceste transformări, ecosistemul mass-mediei s-a confruntat cu o serie de provocări fără precedent în domeniul securității cibernetice. Vulnerabilitățile la atacurile cibernetice, riscurile de compromitere a informațiilor confidențiale și necesitatea de a respecta normele tot mai stricte privind protecția datelor cu caracter personal sunt doar câteva dintre problemele emergente.

Media contemporană, în calitate de actor central în diseminarea informației și formarea opiniei publice, reprezintă o țintă atractivă pentru atacurile cibernetice, fie din partea actorilor politici controversați, fie a grupărilor cibernetice independente. Dinamica tehnologică joacă un rol fundamental în asigurarea securității ecosistemului mediatic, prin dezvoltarea unor soluții inovatoare care să combată aceste amenințări, în mod special în perioadele de criză.

Pe măsură ce noile tehnologii, precum *inteligența artificială*, *blockchain-ul* și *infrastructura cloud* devin tot mai integrate în sectorul media, se impune o reconfigurare a strategiilor de securitate și o adaptare constantă la peisajul de amenințări în continuă schimbare.

Având în vedere caracteristicile specifice spațiului cibernetic, subiectul abordat se află în centrul dezbaterilor din cadrul organizațiilor internaționale, printre care și Alianța Tratatului Atlanticului de Nord (NATO), Comisia Europeană (CE), cu scopul descurajării și răspunsului la așa-numitele activități malițioase care rămân sub pragul unui atac armat. În legătură cu această „zonă gri", NATO a adoptat recent un compendiu privind instrumentele disponibile, care va trebui analizat și dezvoltat din ce în ce mai mult în complementaritate cu instrumente similare aflate sub jurisdicția altor organizații internaționale, în special ale Uniunii Europene (UE).

În circumstanțele actuale, din perspectivă geopolitică, relațiile externe cu alte țări partenere și cu organizații internaționale relevante, precum Organizația Națiunilor Unite (ONU) și Organizația pentru Securitate și Cooperare în Europa (OSCE), în conformitate cu principiile de susținere reciprocă și evitând suprapunerile, constituie o altă dimensiune esențială a activității NATO, destinată să capete o importanță din ce în ce mai mare. Parteneriatele sunt evaluate de la caz la caz și sunt bazate pe valori comune, abordări similare și considerații de interes reciproc, promovate prin intermediul mijloacelor de informare în masă. De o relevanță deosebită este și colaborarea cu sectorul privat, care capătă o importanță majoră în contextul evoluției rapide a amenințărilor, concretizându-se în special prin NATO Industry Cyber Partnership (NICP) [1].

Amenințările cibernetice în mass-media: tendințe și date statistice

Atacurile cibernetice și criminalitatea cibernetică cresc în toată Europa și devin mai complexe. Această tendință se va menține și în viitor, deoarece se preconizează că 41 de miliarde de dispozitive din întreaga lume urmează a fi conectate la Internet până în anul 2025 [2].

Există numeroase rapoarte și statistici care furnizează o perspectivă aprofundată asupra amenințărilor cibernetice specifice domeniului mediatic, precum și asupra evoluției generale a securității cibernetice, evidențiind astfel complexitatea și dinamica riscurilor și măsurilor de protecție în acest sector.

Conform raportului „*Cybersecurity in Media*", publicat de KPMG, în anul 2022 - 44% dintre companiile din sectorul media au experimen-

tat un atac cibernetic semnificativ în ultimii doi ani [3]. Printre principalele vulnerabilități identificate, se numără:

- *Phishing-ul și atacurile de inginerie socială,* care rămân cele mai comune tipuri de atacuri.
- *Atacurile de tip ransomware,* care au devenit o preocupare majoră pentru organizațiile media, având în vedere expunerea pe care o pot crea prin sistarea activităților de producție și distribuție.
- *Riscurile privind protecția datelor.* Unele companii media colectează volume mari de date personale și financiare despre utilizatori, ceea ce le transformă într-o țintă principală pentru atacurile cibernetice.

Un alt studiu în domeniu, „*Verizon Data Breach Investigations Report*" (DBIR), 2023 - oferă date cu privire la tendințele atacurilor cibernetice la nivel global, inclusiv pentru sectorul media. Printre principalele constatări, se numără:

- 73% dintre atacurile cibernetice din mass-media sunt motivate de câștiguri financiare.
- 80% dintre atacurile cibernetice din acest sector implică furtul de date, inclusiv date despre utilizatori, date sensibile și proprietate intelectuală.
- 25% dintre incidentele de compromitere a securității din acest domeniu implică atacuri asupra platformelor de streaming și conținut digital [4].

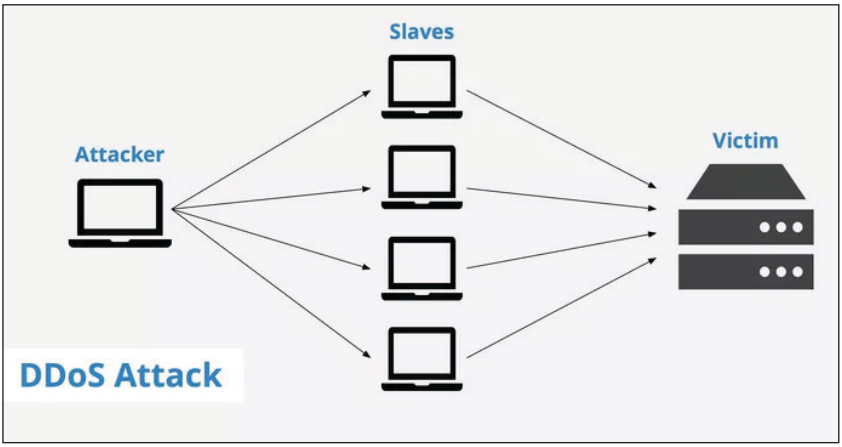
Conform „*Cisco Cybersecurity Readiness Index 2024",* aproape trei sferturi (73%) dintre organizațiile la nivel global consideră că un incident de securitate cibernetică ar putea perturba activitatea lor în următoarele 12 - 24 de luni. Datele publicate arată că 66% dintre aceste organizații intenționează să își revadă strategia de activitate, în mod special din perspectiva revizuirii soluțiilor proiectate pe acest segment, 57% planifică să implementeze soluții noi, iar 55% au în vedere investiții în tehnologii bazate pe Inteligență Artificială (AI) [5].

Extinderea utilizării tehnologiilor informaționale (IT) în procesul de producție și distribuție media a adus noi oportunități, dar și riscuri. În contextul celor menționate anterior, evidențiem și *securitatea conținutului*, care poate fi abordată din perspectiva dezinformării și erodării încrederii publicului în mass-media, dar și cea a piratării, care subminează modelele de afaceri legitime.

Un rol important, în acest sens îl are *European Broadcasting Union* (EBU), care prin activitățile sale de securitate cibernetică în domeniul mass-media își propune să crească gradul de conștientizare și capacitatea de apărare împotriva riscurilor de securitate în continuă evoluție din industrie. EBU reunește experți în securitatea mediatică pentru a face schimb de cunoștințe și experiență pe teme de securitate și pentru a colabora în vederea protejării sistemelor, infrastructurii și procedurilor utilizate în lanțul de producție și distribuție împotriva potențialelor atacuri extrem de dăunătoare. EBU susține că o colaborare între toți actorii din ecosistemul mediatic permite crearea unor mijloace și abordări mai eficiente în lupta împotriva atacurilor cibernetice, pirateriei și dezinformării [6].

Atacurile cibernetice asupra instituțiilor media internaționale și naționale

În ultimii ani, atacurile cibernetice asupra instituțiilor media au devenit tot mai frecvente, afectând grav nu doar fluxul de informații, ci și credibilitatea și siguranța datelor distribuite. Aceste atacuri variază de la *campanii de dezinformare*, *phishing* și *ransomware*, până la atacuri de tip Distributed Denial of Service (DDoS), care întrerup activitatea site-urilor media.



Sursa: Bit2Me Academy. *What are DoS attacks?*
Disponibil: https://academy.bit2me.com/en/which-are-attacks-two/
(accesat: 10.09.2024)

La nivel global, organizații media importante (*Reuters, BBC, The Times, The Daily Mail*, *The Guardian*, *El País*) au fost ținta hackerilor, în special în contexte politice tensionate, cum ar fi alegerile sau conflictele internaționale. Aceste atacuri subliniază nevoia urgentă de măsuri de securitate cibernetică reziliente în protejarea infrastructurii media.

În Republica Moldova, de asemenea, s-au înregistrat cazuri în care platformele media au fost atacate, în special în contextul războiului hibrid și al încercărilor de destabilizare a informațiilor publice. La data de 25 septembrie 2023, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) a confirmat înregistrarea atacului cibernetic asupra anumitor surse de informare, precum: *Nokta* și *Ziarul de Gardă* [7].

În noaptea de 8 spre 9 ianuarie 2024, poșta electronică oficială a postului TV8 a fost expusă unui atac cibernetic. Mai exact, autorii atacului au transmis din numele televiziunii un mesaj către mai multe persoane și instituții, în care pretindeau că un jurnalist din echipa siteului Tv8.md ar fi realizat un interviu cu fondatorul grupului de hackeri DaVinci Group-DVG8873, care se prezintă drept „o forță cibernetică independentă împotriva Ucrainei și a țărilor NATO". Atacul a fost făcut de pe un IP gestionat de pe un host din Amsterdam, Țările de Jos. Proprietarul hostului este compania britanică Aeza International LTD, fondată de un cetățean kazah – Marat Timurov. Aeza International este una dintre cele mai populare companii de hosting din Federația Rusă, iar pe mai multe site-uri de specialitate este prezentată drept o companie rusească [8].

Atacurile de acest tip pot submina credibilitatea instituțiilor media și pot răspândi informații false. Modificarea articolelor sau furtul de materiale sensibile poate afecta grav reputația unei instituții media.

Având un rol principal în informarea publicului și în formarea opiniei publice, mass-media atât cea tradițională, cât și noile media trebuie să elaboreze strategii viabile pentru a face față provocărilor complexe legate de securitatea cibernetică. Furtul de date și compromiterea conținutului sunt amenințări critice care implică accesul neautorizat la baze de date și modificarea sau distrugerea conținutului publicat.

Conchidem, specificând faptul că, în prezent, cele mai frecvente tipuri de atacuri cibernetice asupra instituțiilor media, rămân a fi *DDoS*, care vizează suprasolicitarea serverelor cu un volum masiv de trafic, determinându-le să devină inaccesibile pentru utilizatorii legitimi. Ast-

fel de atacuri pot paraliza site-urile web ale instituțiilor media, afectând negativ accesibilitatea și disponibilitatea informațiilor pentru public. Acestea sunt urmate de *ransomware*, care criptează fișierele instituției și presupun o răscumpărare pentru deblocarea acestora. Atacurile ransomware pot avea efecte devastatoare asupra infrastructurii IT a instituțiilor media, provocând întârzieri în publicarea știrilor și pierderi financiare semnificative. *Phishing-ul* și *social engineering-ul* sunt tehnici utilizate de atacatori pentru a obține informații sensibile prin manipulare. Aceste metode vizează adesea angajații și conducerea instituțiilor media, având ca scop compromiterea conturilor de e-mail și accesul neautorizat la informații confidențiale.

Pentru a face față amenințărilor cibernetice, instituțiile media trebuie să implementeze strategii de protecție și măsuri preventive adecvate. Acestea includ adoptarea unor protocoale de securitate, actualizarea constantă a sistemelor software și educarea angajaților pentru identificarea și raportarea imediată a amenințărilor.

Cele mai frecvente recomandări, în contextul abordării subiectelor privind securitatea cibernetică în domeniul mass-mediei, fie din perspectivă teoretică sau/și practic-aplicativă, se referă la:

- *Sistemele de detecție și răspuns*, care sunt esențiale pentru identificarea rapidă a incidentelor de securitate;
- *Utilizarea de software de monitorizare*, cum ar fi sistemele de detectare a intruziunilor (IDS) și soluțiile de gestionare a evenimentelor de securitate și a informațiilor (SIEM), care permit instituțiilor media să detecteze activitățile suspecte și să răspundă prompt la atacuri;
- *Backup-urile sistematice* și planurile de recuperare sunt măsuri esențiale în cazul unui atac cibernetic;
- *Crearea de copii de siguranță* a datelor importante și testarea acestora sunt indispensabile pentru minimizarea impactului atacurilor ransomware și pentru recuperarea rapidă a operațiunilor.

Măsurile de protecție includ criptarea comunicațiilor, utilizarea autentificării multi-factor și implementarea unor controale stricte de acces. Colaborarea și schimbul de informații cu alte instituții și organizații de securitate cibernetică naționale și internaționale, pot îmbunătăți sistemul de protecție împotriva amenințărilor cibernetice. Aderarea la rețelele de colaborare specializată și partajarea informațiilor despre amenințări și

soluții de securitate, contribuie la întărirea securității cibernetice în industria media.

Referințe bibliografice:

1. Marziali, A. *Cybersecurity: come la NATO si adatta alle nuove sfide*. Disponibil: https://www.ispionline.it/it/pubblicazione/cybersecurity-come-la-nato-si-adatta-alle-nuove-sfide-26627 (accesat: 05.09.2024)
2. Council of the European Union. *Cybersecurity: how the EU tackles cyber threats*. Disponibil: https://www.consilium.europa.eu/en/policies/cybersecurity/ (accesat: 05.09.2024)
3. KPMG Cyber trust insights 2022. *Building trust through cybersecurity and privacy*. Disponibil: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/10/kpmg-cyber-trust -insights-2022.pdf (accesat: 07.09.2024)
4. DBIR *Data Breach Investigations Report 2023*. Disponibil: https://www.verizon.com /business/resources/Tb24/reports/2023-data-breach-investigations-report-dbir.pdf (accesat: 07.09.2024)
5. Cisco Cybersecurity Readiness Index 2024. *Underprepared and overconfident companies tackle an evolving landscape*. Disponibil: https://newsroom.cisco.com/c/dam/r/newsroom / en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_ Readiness_Index_FINAL.pdf (accesat: 07.09.2024)
6. Media Cybersecurity. *Shaping a more secure media industry*. Disponibil: https://tech.ebu.ch/groups/mcs (accesat: 10.09.2024)
7. News Maker. *Mai multe site-uri guvernamentale și de media din Moldova – ținta atacurilor cibernetice.* Precizările autorităților. Disponibil: https://newsmaker.md/ro/mai-multe-site-uri-guvernamentale-si-de-media-din-moldova-tinta-atacurilor-cibernetice-precizarile-autoritatilor/ (accesat: 10.09.2024)
8. Mediacritica. *Poșta electronică oficială a TV8, expusă unui atac cibernetic. Precizările instituției.* Disponibil: https://mediacritica.md/posta-electronica-oficiala-a-tv8-expusa-unui-atac-cibernetic-precizarile-institutiei/ (accesat: 10.09.2024)